Völkerrechtsblog
Der Blog des Arbeitskreises junger Völkerrechtswissenschaftler*innen

DIGITAL SURVEILLANCE AND CYBER ESPIONAGE SYMPOSIUM

The dark side of digitalization

CRISTINA VERONES — 30 November, 2016

It is difficult to imagine today's world without digitalization. We are shopping online, write messages to our friends on WhatsApp, let the world know what we think about a newly elected political leader on Twitter, post a picture of our morning breakfast on Instagram and attend an online-course in "Creative Writing" in the evening. In addition, applications of the "internet of things" silently work around us without us even noticing: the fitness bracelet monitors our pulse and sends the corresponding data concerning our health situation to our iPhone, the fridge independently stocks up on groceries that are about to run out and orders them online and the thermostat is heating the rooms according to the weather forecast on the internet.

Even if not all of these examples apply to each of us, we all leave a vast amount of digital traces, which accumulate to a vast amount of data – so called "big data", which can serve to harvest and identify interesting indications and patterns. In reference to the past activities for extracting something of value, this activity is called "data-mining". It is thus also not surprising that digital data is today often referred to as the "gold" of the future. After the mechanization through water and steam power, the mass production made possible by electrical energy and the use of electronic and IT, we are – it seems – about to witness the 4th industrial revolution.

At least, this is what for example the European Union seems to expect. The European Commission has hence in May 2015 presented its strategy to create a Digital Single Market. By abolishing digital but also physical borders (e.g. for packages), the EU wants to boost its economy and labor market. In addition to the EU, also several States have their "digital strategies", for example, Switzerland, Germany, Sweden, Australia, Mexico and the USA, to name just a few. They all are hopeful that digitalization will lead to progress and development.

Many aspects of digitalization sound more like science-fiction today and all the well-sounding technologies and applications will not have become a reality already by tomorrow. However, the digital and technological development is happening at a very fast pace.

Yet, already today we should not underestimate the "dark sides" of digitalization. In addition to the "digital divide" – the economic and social inequality regarding access, use and impact of information and communication technologies – disadvantages relate especially also to security questions.

From theft and misuse of data, to espionage and cybercrimes – we need to be aware that new technologies also involve risks. Only if people trust these new applications enough, also regarding security aspects, will they embrace them and the "digital revolution" can truly develop to become the newest "industrial" revolution. Thus, States seek to address these hazards with another set of complementary strategies (for example France, Switzerland, Germany, India and the USA) and with ENISA the EU has created a cybersecurity organization at the European Union level.

Yet the aim of more "digital security" risks leading to more digital surveillance and cyberespionage, to the detriment of individuals. The question of the relation of digital surveillance and human rights which we will pursue in the upcoming days is therefore a very topical one. As highlighted before: only if people trust new technologies will they use them in the long run. In the following posts, Christian Djeffel enlightens us on the new problematic dimension of surveillance due to the development of the internet of things, Layla Kristina Jaber writes on the protection of human rights in cyberspace through the European Convention on Human Rights, and Milan Tahraoui concludes with the extraterritorial application of human rights in the digital sphere and asks, whether further developments in this respect will be mainly driven by unilateralism. All three contributions correspond to presentations given at a colloquium on digital surveillance and cyber espionage, which took place in September in Paris.

Cristina Verones (LL.M., PhD) is a member of the editorial team of the Völkerrechtsblog and works as advisor at the Swiss Federal Department of Foreign Affairs (FDFA). The opinions

expressed in this contribution are hers alone and do not reflect the opinion of the FDFA.

Tags: *Cyber*, *Digitalization*, *Human Rights*

Related

In Search of a Shared Grammar: Why Law Is (also) like Poetry.
23 February, 2015
In "Discussion"

Yes, redressing past wrongs in the present!
28 October, 2015
In "Discussion"

The Course of True Law Never Did Run Smooth
24 November, 2014
In "Discussion"

PREVIOUS POST
Towards a more radical deterritorialisation of language

NEXT POST
The surveillance you have paid for

No Comment

Leave a reply

Your email address will not be published. Required fields are marked *

Name (required)

E-Mail (required)

Website

SUBMIT COMMENT

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.